ERDŐS-TURÁN WITH A MOVING TARGET, EQUIDISTRIBUTION OF ROOTS OF REDUCIBLE QUADRATICS, AND DIOPHANTINE QUADRUPLES

GREG MARTIN AND SCOTT SITAR

ABSTRACT. A *Diophantine m-tuple* is a set A of m positive integers such that $ab+1$ is a perfect square for every pair a, b of distinct elements of A. We derive an asymptotic formula for the number of Diophantine quadruples whose elements are bounded by x. In doing so, we extend two existing tools in ways that might be of independent interest. The Erdős-Turán inequality bounds the discrepancy between the number of elements of a sequence that lie in a particular interval modulo 1 and the expected number; we establish a version of this inequality where the interval is allowed to vary. We also adapt an argument of Hooley on the equidistribution of solutions of polynomial congruences to handle reducible quadratic polynomials.

1. INTRODUCTION

A *Diophantine m-tuple* is a set A of m positive integers such that $ab+1$ is a perfect square for every pair a, b of distinct elements of A. For example, the first Diophantine quadruple $\{1, 3, 8, 120\}$ was found by Fermat. (The nomenclature refers to Diophantus, who found a set that has the analogous property in the rational numbers, namely $\{1/16, 33/16, 17/4, 105/16\}$.) It was proved by Dujella [3] that there are no Diophantine sextuples and only finitely many Diophantine quintuples (while a folklore conjecture asserts that there are no Diophantine quintuples at all). However, there are infinitely many Diophantine m-tuples for $2 \le m \le 4$, and thus it is an interesting problem to try to count how many there are beneath a given bound.

Dujella showed [2] that the number of Diophantine pairs contained in $[1, x]$ is asymptotic to $\frac{6}{\pi^2} x \log x$, while the number of Diophantine triples contained in $[1, x]$ is asymptotic to $\frac{3}{\pi^2} x \log x$. He considered the same counting problem for Diophantine quadruples, obtaining for sufficiently large x the lower and upper bounds $0.1608 x^{1/3} \log x$ and $0.5354 x^{1/3} \log x$, respectively, for the number of Diophantine quadruples contained in $[1, x]$. The primary purpose of this paper is to establish the following asymptotic formula:

Theorem 1.1. *The number of Diophantine quadruples contained in $[1, x]$ is given by the asymptotic formula*

$$C x^{1/3} \log x + O\big(x^{1/3} (\log x)^{2/3+\sqrt{2}/6} (\log\log x)^{5/12}\big),$$

where $C = 2^{4/3}/3\Gamma(\frac{2}{3})^3 \approx 0.338285$.

Note that the exponent of $\log x$ in the error term, $\frac{2}{3} + \frac{\sqrt{2}}{6} \approx 0.90237$, is indeed slightly smaller than 1.

In the course of establishing Theorem 1.1, we found ourselves needing to extend two existing tools from the literature to suit our needs; these extensions might be of interest in their own right. The first of these tools is the Erdős-Turán inequality, which gives a quantitative bound for the discrepancy between the number of elements of a sequence that lie in a particular interval modulo 1

2000 *Mathematics Subject Classification.* Primary 11D45, 11N45; secondary 11K06, 11K38.

and the expected number. We require a version of this inequality in which the target interval is allowed to vary. To set some notation, let $u = \{u_n\}$, $\alpha = \{\alpha_n\}$, and $\beta = \{\beta_n\}$ be sequences of real numbers; we are interested in counting how many elements u_n lie in the corresponding interval $[\alpha_n, \beta_n]$ modulo 1. (So that these intervals modulo 1 are sensible, we make the restriction $\alpha_n \le \beta_n \le \alpha_n + 1$ for all n.) Define the counting function

$$Z_N = Z_N(u; \alpha, \beta) = \#\{1 \le n \le N : u_n \in [\alpha_n, \beta_n] \pmod 1\} \tag{1}$$

and the discrepancy between the counting function and the expected number

$$D_N = D_N(u; \alpha, \beta) = Z_N - \sum_{n=1}^{N} (\beta_n - \alpha_n). \tag{2}$$

For any sequence $\{s_n\}$, let $V_N(s) = \sum_{n=1}^{N-1} \|s_{n+1} - s_n\|$ denote its total variation considered as a sequence modulo 1, where $\|y\| = \min_{z \in \mathbb{Z}} |y - z|$ is the natural metric on $\mathbb{R}/\mathbb{Z}$. We prove the following "moving target" extension of the Erdős–Turán inequality in Section 2.

Theorem 1.2. *Let $\{u_n\}$, $\{\alpha_n\}$, and $\{\beta_n\}$ be sequences of real numbers with $\alpha_n \le \beta_n \le \alpha_n + 1$. With $D_N = D_N(u; \alpha, \beta)$ as defined as in equation* (2)*, we have*

$$|D_N| \le \frac{N}{H+1} + \sum_{h=1}^{H} \big(1 + \pi h (V_N(\alpha) + V_N(\beta))\big) \left(\frac{2-c}{H+1} + \frac{c}{h} \right) M_N(h) \tag{3}$$

for any positive integers N and H, where $c = 16/7\pi$ and

$$M_N(h) = \max_{1 \le T \le N} \left| \sum_{n=1}^{T} e(h u_n) \right|. \tag{4}$$

The following corollary is an immediate consequence of Theorem 1.2 and is easy to apply in many concrete situations.

Corollary 1.3. *Let $\{u_n\}$, $\{\alpha_n\}$, and $\{\beta_n\}$ be sequences of real numbers with $\alpha_n \le \beta_n \le \alpha_n + 1$. Suppose that both α and β are monotone sequences. With $D_N = D_N(u; \alpha, \beta)$ as defined as in equation* (2)*, we have*

$$|D_N| \ll \frac{N}{H} + \big(1 + |\alpha_N - \alpha_1| + |\beta_N - \beta_1|\big) \sum_{h=1}^{H} M_N(h)$$

for any positive integers N and H, where $M_N(h)$ is defined in equation (4)*.*

We compare our Theorem 1.2 to the standard Erdős–Turán inequality, and exhibit two examples that probe the sharpness of our inequality, at the end of Section 2.

The second tool that we extend is a result of Hooley on the equidistribution of the roots of polynomial congruences. Specifically, given any polynomial $f(t) \in \mathbb{Z}[t]$, we consider the sequence of real numbers $\frac{\nu}{k}$, where k runs over all positive integers up to some bound y and ν runs, for each k, over the roots of the congruence $f(\nu) \equiv 0 \pmod k$. Corresponding to such a sequence, we define the exponential sum

$$R_f(h, y) = \sum_{k \le y} \sum_{\substack{f(\nu) \equiv 0 \pmod k \\ 0 < \nu \le k}} e^{2\pi i h \nu / k}. \tag{5}$$

Hooley [4, 5] established nontrivial upper bounds for $R_f(h,y)$ when f is an irreducible polynomial of degree at least 2. By adapting the methods of [4], we prove the following analogous upper bound for reducible quadratic polynomials in Section 3.

Theorem 1.4. *Let f be a reducible, nonsquare quadratic polynomial with integer coefficients, and let D be its discriminant. Let $R_f(h,y)$ be defined as in equation* (5)*. For all real numbers $y \geq 3$ and for every integer $h \neq 0$,*

$$R_f(h,y) \ll \sqrt{D} \prod_{p|h} \left(1 + \frac{7}{\sqrt{p}}\right) \cdot y(\log y)^{\sqrt{2}-1} (\log\log y)^{5/2}.$$

The trivial bound for $R_f(h,x)$, namely the number of summands, has order of magnitude $y \log y$ (see Lemma 5.5), and so Theorem 1.4 represents a nontrivial upper bound for the sum when y is sufficiently large. It follows immediately from Weyl's criterion [7, page 1] that the normalized roots ν/k are equidistributed modulo 1. We remark that for reducible quadratic polynomials f, the true order of magnitude of $R_f(h,y)$ is probably y; therefore the estimate in Theorem 1.4 cannot be improved too much. We discuss these issues further in Section 3.

In Section 4 we show how these two tools can be used to prove Theorem 1.1. Several times in Sections 3 and 4, we need to invoke standard results on sums of multiplicative functions; to preserve the flow of ideas, we defer the proofs of all such results to Section 5.

2. Erdős-Turán with a moving target

In this section we prove Theorem 1.2. We begin by recalling the standard approach to bounding the discrepancy D_N using exponential sums and Selberg's "magic functions". We then derive a bound for the individual Fourier coefficients that arise when using Selberg's functions. At that point, we can use partial summation to finish the proof of Theorem 1.2. At the end of the section, we compare our "moving target" inequality to the standard Erdős–Turán inequality and exhibit two examples that probe the sharpness of our inequality.

2.1. Bounding the discrepancy by exponential sums.

We begin by defining, for any positive integer H, the trigonometric polynomial of degree H

$$B_H(x) = \frac{1}{H+1} \sum_{h=1}^{H} f\left(\frac{h}{H+1}\right) \sin 2\pi hx + \frac{1}{2(H+1)} \sum_{h=-H}^{H} \left(1 - \frac{|h|}{H+1}\right) e(hx), \tag{6}$$

where $e(y) = e^{2\pi i y}$ as usual and

$$f(y) = -(1-y)\cot \pi y - \tfrac{1}{\pi}. \tag{7}$$

We have $\hat{B}_H(0) = 1/(2(H+1))$ and $\hat{B}_H(h) = 0$ if $|h| \geq H+1$, while if $1 \leq h \leq H$ then

$$\hat{B}_H(\pm h) = \frac{1}{2(H+1)} \left(1 - \frac{|h|}{H+1} \mp i f\left(\frac{|h|}{H+1}\right)\right). \tag{8}$$

We then define, for any real numbers α and β satisfying $\alpha \leq \beta \leq \alpha + 1$, the two related trigonometric polynomials

$$S_H^+(\alpha,\beta;y) = \beta - \alpha + B_H(y-\beta) + B_H(\alpha - y)$$
$$S_H^-(\alpha,\beta;y) = \beta - \alpha - B_H(\beta - y) - B_H(y-\alpha),$$

which satisfy $\hat{S}_H^{\pm}(0) = \beta - \alpha \pm 1/(H+1)$ and, for $h \neq 0$,

$$\begin{aligned} \hat{S}_H^+(h) &= \hat{B}_H(h)e(-h\beta) + \hat{B}_H(-h)e(h\alpha) \\ \hat{S}_H^-(h) &= -\hat{B}_H(-h)e(h\beta) - \hat{B}_H(h)e(-h\alpha). \end{aligned} \tag{9}$$

These trigonometric polynomials are useful one-sided approximants to the characteristic function $\chi(\alpha, \beta; y)$ of the interval $[\alpha, \beta]$ modulo 1, which equals 1 if there is some number z between α and β such that $y \equiv z \pmod 1$ and 0 otherwise:

Proposition 2.1. *For any real numbers α and β satisfying $\alpha \leq \beta \leq \alpha + 1$,*

$$S_H^-(\alpha, \beta; y) \leq \chi(\alpha, \beta; y) \leq S_H^+(\alpha, \beta; y)$$

for all real numbers y.

Proof. This is the fundamental property of the "Selberg magic functions" $S_H^{\pm}$; see [7, chapter 1] for an exposition which uses the notation we have employed. □

Note that the definition (1) of Z_N can be written as $Z_N = \sum_{n \leq N} \chi(\alpha_n, \beta_n; u_n)$. Following the approach to proving the standard Erdős–Turán inequality, we use Proposition 2.1 to write the upper bound

$$Z_N \leq \sum_{n \leq N} S_H^+(\alpha_n, \beta_n; u_n) = \sum_{n \leq N} \left(\beta_n - \alpha_n + \frac{1}{H+1} + \sum_{1 \leq |h| \leq H} \hat{S}_H^+(h) e(hu_n) \right)$$

(where we have singled out the constant term $\hat{S}_H^+(0)$ of S_H^+); the definition (2) of D_N thus yields

$$\begin{aligned} D_N &\leq \frac{N}{H+1} + \sum_{n \leq N} \sum_{1 \leq |h| \leq H} \hat{S}_H^+(h) e(hu_n) \\ &= \frac{N}{H+1} + \sum_{n \leq N} \sum_{1 \leq |h| \leq H} \big(\hat{B}_H(h) e(-h\beta_n) + \hat{B}_H(-h) e(h\alpha_n) \big) e(hu_n) \end{aligned}$$

by equation (9). Interchanging the order of summation, we get

$$D_N \leq \frac{N}{H+1} + \sum_{1 \leq |h| \leq H} \left(\hat{B}_H(h) \sum_{n \leq N} e(hu_n) e(-h\beta_n) + \hat{B}_H(-h) \sum_{n \leq N} e(hu_n) e(h\alpha_n) \right). \tag{10}$$

The same calculation using S_H^- instead of S_H^+ yields the corresponding lower bound

$$D_N \geq -\frac{N}{H+1} - \sum_{1 \leq |h| \leq H} \left(\hat{B}_H(-h) \sum_{n \leq N} e(hu_n) e(h\beta_n) + \hat{B}_H(h) \sum_{n \leq N} e(hu_n) e(-h\alpha_n) \right). \tag{11}$$

If the sequences α and β were constant, as in the standard Erdős–Turán inequality, then we could now factor out the exponential sum $\sum_{n \leq N} e(hu_n)$ and then bound the remaining sum over h at once. Instead, we bound the Fourier coefficients $\hat{B}_H(h)$ individually and use partial summation to estimate the effect of the varying terms $e(-h\beta_n)$ and $e(-h\alpha_n)$ on the exponential sums.

2.2. **Bounding the Fourier coefficients.** We begin by establishing an inequality between the cotangent function and a rational function that we will use to bound the function f from the previous section.

Lemma 2.2. *For $0 < y < 1$, we have*

$$\pi \cot \pi y + \frac{1}{1-y} < \frac{1}{y} + \frac{3(1-y)}{2} - \frac{1}{2-y}.$$

Proof. We start with the classical equality [1, equation (4.3.91)]

$$\begin{aligned}\pi \cot \pi z &= \frac{1}{z} + \sum_{\substack{n\in\mathbb{Z}\\ n\neq 0}} \left(\frac{1}{z+n} - \frac{1}{n}\right) \\ &= \frac{1}{z} + \frac{1}{z+1} + \frac{1}{z-1} - 2z\sum_{n=2}^{\infty} \frac{1}{n^2 - z^2} \\ &> \frac{1}{z} + \frac{1}{z+1} + \frac{1}{z-1} - 2z\sum_{n=2}^{\infty} \frac{1}{n^2 - 1} = \frac{1}{z} + \frac{1}{z+1} + \frac{1}{z-1} - \frac{3z}{2},\end{aligned}$$

where the inequality is valid for $|z| < 1$. Substituting $z = 1 - y$ yields

$$-\pi \cot \pi y = \pi \cot(\pi(1-y)) > \frac{1}{1-y} + \frac{1}{2-y} - \frac{1}{y} - \frac{3(1-y)}{2},$$

which is equivalent to the statement of the lemma. □

Lemma 2.3. *Let f be defined as in equation* (7)*. For $0 < y < 1$, we have $|f(y)| < \frac{c}{2}\left(\frac{1}{y} - 1\right)$, where $c = \frac{16}{7\pi}$.*

Proof. It is equivalent to show that

$$\frac{\pi|f(y)|}{1-y} - \frac{8}{7y} < 0$$

for $0 < y < 1$. By Lemma 2.2, we have

$$\begin{aligned}\frac{\pi|f(y)|}{1-y} - \frac{8}{7y} &= \left(\pi \cot \pi y + \frac{1}{1-y}\right) - \frac{8}{7y} \\ &< \left(\frac{1}{y} + \frac{3(1-y)}{2} - \frac{1}{2-y}\right) - \frac{8}{7y} = \frac{21y^3 - 63y^2 + 30y - 4}{14y(2-y)}.\end{aligned}$$

The denominator of the right-hand side is obviously positive for $0 < y < 1$; it suffices to show that the numerator is negative in that range. The polynomial $p(t) = 21t^3 - 63t^2 + 30t - 4$ has negative discriminant $-29{,}484$, and so it has exactly one real root. Moreover, $p(1) = -16$ and $\lim_{y\to\infty} p(y) = \infty$, so that real root is greater than 1; in particular, $p(y) < 0$ for all $y < 1$. □

We are now able to bound the Fourier coefficients $\hat{B}_H(h)$.

Lemma 2.4. *Let B_H be defined as in equation* (6)*. For $h \neq 0$, we have*

$$\left|\hat{B}_H(h)\right| < \frac{1}{4}\left(\frac{2-c}{H+1} + \frac{c}{|h|}\right),$$

where $c = \frac{16}{7\pi}$.

Proof. From the formula (8) for the Fourier coefficients of B_H, we see that

$$\begin{aligned}\big|\hat{B}_H(h)\big| &= \frac{1}{2(H+1)}\left(\left(1-\frac{|h|}{H+1}\right)^2 + f\left(\frac{|h|}{H+1}\right)^2\right)^{1/2} \\ &\le \frac{1}{2(H+1)}\left(1-\frac{|h|}{H+1}+\left|f\left(\frac{|h|}{H+1}\right)\right|\right) \\ &< \frac{1}{2(H+1)}\left(1+\frac{c}{2}\left(\frac{1-|h|/(H+1)}{|h|/(H+1)}\right)\right)\end{aligned} \tag{12}$$

by Lemma 2.3; this inequality is equivalent to the statement of the lemma. □

2.3. **Finishing the proof of Theorem 1.2.** At this point, we need only to record the outcome of a partial summation argument to be fully prepared to prove Theorem 1.2. Recall that $V_N(s) = \sum_{n=1}^{N-1} \|s_{n+1} - s_n\|$ denotes the total variation modulo 1 of the sequence $s = \{s_n\}$.

Lemma 2.5. *For any sequences $\{u_n\}$ and $\{s_n\}$ of real numbers and for any integer h,*

$$\left|\sum_{n=1}^{N} e(hu_n)e(-hs_n)\right| \le \big(1+2\pi|h|V_N(s)\big)M_N(h),$$

where $M_N(h)$ is defined in equation (4)*.*

Proof. Let $E_T(h) = \sum_{n=1}^{T} e(hu_n)$. Using partial summation, we have

$$\begin{aligned}\sum_{n=1}^{N} e(hu_n)e(-hs_n) &= \sum_{n=1}^{N}\big(E_n(h)-E_{n-1}(h)\big)e(-hs_n) \\ &= E_N(h)e(-hs_N) - \sum_{n=1}^{N-1} E_n(h)(e(-hs_{n+1})-e(-hs_n)),\end{aligned}$$

and so by the triangle inequality

$$\begin{aligned}\left|\sum_{n=1}^{N-1} e(hu_n)e(-hs_n)\right| &\le |E_N(h)| + \sum_{n=1}^{N-1}|E_n(h)|\cdot|e(-hs_{n+1})-e(-hs_n)| \\ &\le M_N(h)\left(1+\sum_{n=1}^{N-1}|e(-hs_{n+1})-e(-hs_n)|\right).\end{aligned}$$

From elementary properties of the exponential function,

$$|e(-hs_{n+1})-e(-hs_n)| = \big|1-e\big(h(s_{n+1}-s_n)\big)\big| = \big|1-e\big(h\|s_{n+1}-s_n\|\big)\big|;$$

furthermore, $|1-e(y)| \le 2\pi|y|$ by the mean value theorem. We conclude that

$$\left|\sum_{n=1}^{N-1} e(hu_n)e(-hs_n)\right| \le M_N(h)\left(1+2\pi|h|\sum_{n=1}^{N-1}\|s_{n+1}-s_n\|\right),$$

which establishes the lemma. □

Proof of Theorem 1.2. Beginning with the upper bound (10) on D_N,

$$D_N \le \frac{N}{H+1} + \sum_{1\le|h|\le H}\left(\hat{B}_H(h)\sum_{n\le N} e(hu_n)e(-h\beta_n) + \hat{B}_H(-h)\sum_{n\le N} e(hu_n)e(h\alpha_n)\right),$$

we use Lemma 2.4 to obtain

$$D_N \le \frac{N}{H+1} + \sum_{1\le|h|\le H}\frac{1}{4}\left(\frac{2-c}{H+1}+\frac{c}{|h|}\right)\left(\left|\sum_{n\le N} e(hu_n)e(-h\beta_n)\right| + \left|\sum_{n\le N} e(hu_n)e(h\alpha_n)\right|\right).$$

where $c = \frac{16}{7\pi}$. We now invoke Lemma 2.5 to see that

$$\begin{aligned} D_N &\le \frac{N}{H+1} \\ &\qquad + \sum_{1\le|h|\le H}\frac{1}{4}\left(\frac{2-c}{H+1}+\frac{c}{|h|}\right)\Big(\big(1+2\pi|h|V_N(\beta)\big)M_N(-h) + \big(1+2\pi|h|V_N(\alpha)\big)M_N(h)\Big) \\ &\le \frac{N}{H+1} + \frac{1}{4}\sum_{1\le|h|\le H}\left(\frac{2-c}{H+1}+\frac{c}{|h|}\right)\big(2+2\pi|h|(V_N(\alpha)+V_N(\beta))\big)M_N(h), \end{aligned}$$

since $M_N(-h) = M_N(h)$. At this point the summands for h and $-h$ are equal, and so

$$D_N \le \frac{N}{H+1} + \sum_{h=1}^{H}\left(\frac{2-c}{H+1}+\frac{c}{h}\right)\big(1+\pi h(V_N(\alpha)+V_N(\beta))\big)M_N(h).$$

This is precisely the upper bound claimed in the statement of Theorem 1.2; the lower bound is established by exactly the same proof, starting with the lower bound (11) on D_N. □

2.4. **Probing the sharpness of Theorem 1.2.** The standard Erdős–Turán inequality [7, equation (23)] has the form

$$|D_N| \le \frac{N}{H+1} + \sum_{h=1}^{H}\left(\frac{2}{H+1} + \min\left\{\beta-\alpha, \frac{2/\pi}{h}\right\}\right)\left|\sum_{n=1}^{N} e(hu_n)\right|.$$

If we restrict α and β to be constant sequences in Theorem 1.2, the conclusion is that

$$\begin{aligned} |D_N| &\le \frac{N}{H+1} + \sum_{h=1}^{H}\left(\frac{2-c}{H+1}+\frac{c}{h}\right)M_N(h) \\ &= \frac{N}{H+1} + \sum_{h=1}^{H}\left(\frac{2-c}{H+1}+\frac{c}{h}\right)\max_{1\le T\le N}\left|\sum_{n=1}^{T} e(hu_n)\right|. \end{aligned}$$

In theory, this conclusion is weaker than the traditional Erdős–Turán inequality due to the presence of the maximum; in practice, however, the attainable bounds on the exponential sums that arise are increasing functions of T, and so nothing would be lost. (Our method also does not include the possibility of replacing the $\frac{c}{h}$ with $\beta-\alpha$, as the latter difference is not independent of n.)

Moreover, in its full "moving target" generality, the term $M_N(h)$ in Theorem 1.2 cannot be replaced by $\left|\sum_{n=1}^{N} e(hu_n)\right|$. To see this, we consider the sequence $\{u_n\} = \{n/(N+1)\}$ for some positive integer N, and we select the "obliging target" intervals bounded by the sequences

$$\{\alpha_n\} = \{u_n - 2^{-n}\} \quad \text{and} \quad \{\beta_n\} = \{u_n + 2^{-n}\}. \tag{13}$$

The total lengths of these intervals is bounded by 2, but the number of points in the sequence u that lie in the intervals $[\alpha, \beta]$ is N; therefore $D_N \geq N - 2$ in this situation. However, the total variations of the sequences α and β are bounded by $\frac{3}{2}$, while the exponential sum $\sum_{n=1}^{N} e(hu_n) = \sum_{n=1}^{N} e(hn/(N+1))$ has the exact value of -1 for every integer $1 \leq h \leq N$. Therefore, for any integer H between 1 and N,

$$\frac{N}{H+1} + \sum_{h=1}^{H} \bigl(1 + \pi h(V_N(\alpha) + V_N(\beta))\bigr)\left(\frac{2-c}{H+1} + \frac{c}{h}\right)\left|\sum_{n=1}^{N} e(hu_n)\right| < \frac{N}{H+1} + \sum_{h=1}^{H}(1+3\pi h)\left(\frac{2-c}{H+1} + \frac{c}{h}\right) \ll \frac{N}{H} + H.$$

Since the right-hand side can be substantially smaller than $N - 2$ (when H is near $\sqrt{N}$, for instance), it is impossible for the left-hand side to be an upper bound for D_N. Theorem 1.2 remains valid in this situation, though, since $M_N(h)$ is approximately $\frac{N}{h}$, whence the right-hand side of equation (3) has order of magnitude $N \log H$.

We can also consider the sequence $\{u_n\} = \{n^\gamma\}$ for some real number $0 < \gamma < 1$ and the same "obliging intervals" (13) as before, so that the discrepancy is again at least $N - 2$. The terms on the right-hand side of equation (3) must therefore conspire to give a contribution whose order of magnitude is at least N. The total variations of α and β are each $N^\gamma + O(1)$, while the exponential sum $\sum_{n=1}^{N} e(hn^\gamma)$ can be shown to be asymptotic to $N^{1-\gamma} e(hN^\gamma)/(2\pi i h\gamma)$, which has order of magnitude $N^{1-\gamma}/h$. Therefore the right-hand side of equation (3) has order of magnitude

$$\frac{N}{H} + \sum_{h=1}^{H} N^\gamma \frac{N^{1-\gamma}/h}{h} \sim N \log H,$$

showing that the bound is both correct and reasonably tight in this case as well.

Both of these examples provide extremely positive discrepancies D_N, but simply replacing the "obliging intervals" $[\alpha_n, \beta_n]$ with their complements $[\beta_n, \alpha_n + 1]$ yields extremely negative disrepancies instead.

Different methods of bounding the Fourier coefficients $\hat{B}_H(h)$ yield different constants, in equation (3), in the numerators of the fractions whose denominators are $H+1$ and h. The constants $2-c$ and c we have derived above compare favorably to the constants yielded by other methods. Still, we can immediately identify two ways one could improve these constants if such an improvement were desired. First, the constant $\frac{c}{2}$ in Lemma 2.3 is approximately 0.363783; from a numerical study, the best possible constant in this part of the argument would be approximately 0.356113, a difference of about 2%. Even aside from this, both of the inequalities in equation (12) can be noticeably improved for $|h|$ near H by elementary means.

3. Equidistribution of roots of quadratic congruences

Our goal here is to modify the argument in Hooley's paper to show that the roots of a reducible quadratic are equidistributed in the same sense as his paper.

3.1. **Number of roots of reducible quadratics.**

For any polynomial f with integer coefficients, define

$$\rho_f(m) = \#\{1 \leq r \leq m\colon\ f(r) \equiv 0 \pmod{m}\}$$

to be the number of roots of $f \pmod m$ in a block of m consecutive integers. By the Chinese remainder theorem, the function ρ_f is multiplicative for any f. We also use the common notation $\mathrm{ord}_p(n)$ to denote the multiplicity with which the prime p divides n, and we write $p^\alpha \parallel n$ when $\mathrm{ord}_p(n) = \alpha$.

Recall that the *content* of a polynomial with integer coefficients is the greatest common divisor of its coefficients. A polynomial with integer coefficients is called *primitive* if its content equals 1. Our first lemma allows us to reduce the task of counting roots of polynomials $\pmod m$ to the primitive case.

Lemma 3.1. *Given $f(t) \in \mathbb{Z}[t]$, let W be the content of f and write $g(t) = \frac{1}{W} f(t) \in \mathbb{Z}[t]$. Let p be a prime, and let $\gamma = \mathrm{ord}_p(W)$. Then for any positive integer α,*

$$\rho_f(p^\alpha) = \begin{cases} p^\alpha, & \text{if } \alpha \le \gamma, \\ p^\gamma \rho_g(p^{\alpha-\gamma}), & \text{if } \alpha > \gamma. \end{cases}$$

Proof. The congruence $f(r) = Wg(r) \equiv 0 \pmod m$ is equivalent [8, Theorem 2.3(1)] to $g(r) \equiv 0 \pmod{\frac{m}{(W,m)}}$. When $m = p^\alpha$ with $\alpha \le \gamma$, then $(W, m) = p^\alpha$ and the congruence is equivalent to $g(r) \equiv 0 \pmod 1$; this is satisfied by every integer, in particular by all p^α of the integers between 1 and p^α. When $m = p^\alpha$ with $\alpha > \gamma$, then $(W, m) = p^\gamma$ and the congruence is equivalent to $g(r) \equiv 0 \pmod{p^{\alpha-\gamma}}$; this is satisfied by $\rho_g(p^{\alpha-\gamma})$ integers in every block of $p^{\alpha-\gamma}$ consecutive integers, in particular by $p^\gamma \rho_g(p^{\alpha-\gamma})$ of the integers between 1 and p^α. □

In our investigation of the values of ρ_g for primitive reducible quadratics g, we will need the following elementary but awkward result.

Lemma 3.2. *Fix integers α and δ. Suppose that y and z are integers satisfying either*

(i) $y = z < \delta$ *or*
(ii) $\min\{y, z\} = \delta$.

If $\alpha \le 2\delta$, then the inequality $y + z \ge \alpha$ is equivalent to $y \ge \lceil \frac{\alpha}{2} \rceil$, while if $\alpha > 2\delta$, then the inequality $y + z \ge \alpha$ is equivalent to the conjunction

$$\min\{y, z\} = \delta \text{ and } \max\{y, z\} \ge \alpha - \delta.$$

Proof. We begin by assuming that $\alpha \le 2\delta$. First suppose that $y \ge \lceil \frac{\alpha}{2} \rceil$, which is equivalent to $y \ge \frac{\alpha}{2}$ since y is an integer. If (i) holds, then indeed $y + z = 2y \ge \alpha$; while if (ii) holds, then $y + z \ge y + \delta \ge \frac{\alpha}{2} + \frac{\alpha}{2} = \alpha$. On the other hand, suppose that $y < \lceil \frac{\alpha}{2} \rceil$, which is equivalent to $y < \frac{\alpha}{2}$. If (i) holds, then $y + z = 2y < \alpha$; while (ii) is impossible due to the contradiction $y < \frac{\alpha}{2} \le \delta = \min\{y, z\} \le y$. This establishes the first asserted equivalence.

Now we assume that $\alpha > 2\delta$. The condition (i) forces both $y + z < 2\delta < \alpha$ and $\min\{y, z\} < \delta$, which makes both sides of the second asserted equivalence false. On the other hand, under condition (ii) the inequalities $y + z \ge \alpha$ and $\max\{y, z\} \ge \alpha - \delta$ are equivalent, since $y + z = \min\{y, z\} + \max\{y, z\}$. This establishes the second asserted equivalence. □

Any primitive reducible quadratic can be written as $g(t) = (at+b)(ct+d)$, where the primitivity implies that $(a, b) = (c, d) = 1$. Define $\Delta = |ad - bc|$, and note that the discriminant of g equals Δ^2. We note that g is the square of a linear polynomial if and only if $\Delta = 0$.

Lemma 3.3. *Let $g(t) = (at + b)(ct + d)$ where $a, b, c, d \in \mathbb{Z}$ and $(a, b) = (c, d) = 1$, and define $\Delta = |ad - bc|$. Assume that $\Delta \neq 0$. Let p be a prime, and let $\delta = \mathrm{ord}_p(\Delta)$. Then for any positive integer α,*

$$\rho_g(p^\alpha) = \begin{cases} 2, & \text{if } p \nmid ac\Delta, \\ 0, & \text{if } p \mid ac \text{ and } p \mid \Delta, \\ 1, & \text{if } p \mid ac \text{ and } p \nmid \Delta, \\ p^{\lfloor \alpha/2 \rfloor}, & \text{if } p \nmid ac \text{ and } p \mid \Delta \text{ and } \alpha \leq 2\delta, \\ 2p^\delta, & \text{if } p \nmid ac \text{ and } p \mid \Delta \text{ and } \alpha > 2\delta. \end{cases} \tag{14}$$

In particular, $\rho_g(p^\alpha) \leq 2p^\delta$.

We remark that since $(a, b) = (c, d) = 1$, any prime that divides two of a, c, and Δ automatically divides the third. Therefore the second line of the formula (14) is the case where p divides both of a and c, while the third line is the case where p divides exactly one of a and c.

Proof. First suppose that p divides both a and c. Then the congruence $g(r) \equiv 0 \pmod{p^\alpha}$ implies $bd \equiv 0 \pmod{p}$, which is a contradiction since $(a, b) = (c, d) = 1$. Therefore $\rho_g(p^\alpha) = 0$ in this case.

Next suppose that $p \nmid \Delta$. Since Δ is an integer linear combination of $ar + b$ and $cr + d$ for any integer r, it is impossible for p to divide both such integers simultaneously. Thus the number of roots of $g(r) \equiv 0 \pmod{p^\alpha}$ is simply the sum of the numbers of roots of $ar + b \equiv 0 \pmod{p^\alpha}$ and $cr + d \equiv 0 \pmod{p^\alpha}$. The number of roots modulo p^α of $ar + b \equiv 0 \pmod{p^\alpha}$ is 1 if $p \nmid a$ and 0 if $p \mid a$ (since $p \nmid b$ in the second case), and similarly for the number of roots modulo p^α of $cr + d \equiv 0 \pmod{p^\alpha}$. Therefore $\rho_g(p^\alpha)$ equals 1 if p divides exactly one of a and c and 2 if it divides neither.

Having disposed of the first three cases, for the rest of the proof we may assume that $p \nmid ac$ and $p \mid \Delta$ (so that $\delta \geq 1$). The congruence $g(r) \equiv 0 \pmod{p^\alpha}$ is then equivalent to $(r + ba^{-1})(r + dc^{-1}) \equiv 0 \pmod{p^\alpha}$. We may translate r without affecting the number of roots modulo p^α, so it is equivalent to look at the congruence $r(r + \Delta_1) \equiv 0 \pmod{p^\alpha}$, where $\Delta_1 = dc^{-1} - ba^{-1} = \pm\Delta/ac$. To calculate $\rho_g(p^\alpha)$, we thus need to count the number of integers $1 \leq r \leq p^\alpha$ such that $\mathrm{ord}_p(r) + \mathrm{ord}_p(r + \Delta_1) \geq \alpha$.

Note that $p^\delta \parallel \Delta_1$ as well (meaning that p^δ exactly divides its numerator while p does not divide its denominator). The p-adic ultrametric inequality tells us that of the three numbers $\{\mathrm{ord}_p(r), \mathrm{ord}_p(r + \Delta_1), \delta\}$, the two smallest are equal (or all three are equal). This implies that for any integer r, exactly one of the following situations holds:

- $\mathrm{ord}_p(r) = \mathrm{ord}_p(r + \Delta_1) < \delta$; or
- $\min\{\mathrm{ord}_p(r), \mathrm{ord}_p(r + \Delta_1)\} = \delta$.

If $\alpha \leq 2\delta$, we apply Lemma 3.2 to see that $\mathrm{ord}_p(r) + \mathrm{ord}_p(r + \Delta_1) \geq \alpha$ exactly when $\lceil \frac{\alpha}{2} \rceil \leq \mathrm{ord}_p(r)$. The number of such r between 1 and p^α is just the number of multiples of $p^{\lceil \alpha/2 \rceil}$ in that range, which is exactly $p^\alpha / p^{\lceil \alpha/2 \rceil} = p^{\lfloor \alpha/2 \rfloor}$. This settles the fourth case.

On the other hand, if $\alpha \leq 2\delta$, we apply Lemma 3.2 to see that $\min\{\mathrm{ord}_p(r), \mathrm{ord}_p(r + \Delta_1)\} = \delta$ and $\max\{\mathrm{ord}_p(r), \mathrm{ord}_p(r + \Delta_1)\} \geq \alpha - \delta > \delta$. For such integers r, either r or $r + \Delta_1$ must be a multiple of $p^{\alpha - \delta}$ (and not both, since $\alpha - \delta > \delta$). The number of such r between 1 and p^α is therefore exactly $2p^\alpha / p^{\alpha - \delta} = 2p^\delta$. This settles the fifth and final case. □

Lemma 3.4. *Let f be a reducible, nonsquare quadratic polynomial with integer coefficients, and let D be its discriminant. Then $\rho(m) \leq \sqrt{D} \cdot 2^{\omega(m)}$.*

Proof. Note that $D \neq 0$ since g is not the square of a linear polynomial by assumption. As noted earlier in this section, we can write $f(t) = W(at+b)(ct+d)$ for some integers W, a, b, c, d with $(a,b) = (c,d) = 1$. Let p be any prime, and let $\beta = \operatorname{ord}_p(\sqrt{D})$, which is an integer since D is a perfect square. Choose γ and δ such that $p^\gamma \parallel W$ and $p^\delta \parallel (ad-bc)$, so that $\gamma + \delta = \beta$. If $\alpha \leq \gamma$, then Lemma 3.1 tells us that $\rho_f(p^\alpha) = p^\alpha \leq p^\gamma \leq p^\beta$. If $\alpha > \gamma$, then Lemmas 3.1 and 3.3 tell us that $\rho_f(p^\alpha) = p^\gamma \rho_f(p^{\alpha-\gamma}) \leq p^\gamma \cdot 2p^\delta = 2p^\beta$. In either case we see that $\rho_f(p^\alpha) \leq 2p^{\operatorname{ord}_p(\sqrt{D})}$. Then, since ρ_f is multiplicative,

$$\rho_f(m) = \prod_{p^\alpha \| m} \rho_f(p^\alpha) \leq \prod_{p|m} \left(2p^{\operatorname{ord}_p(\sqrt{D})}\right) = \prod_{p|m} p^{\operatorname{ord}_p(\sqrt{D})} \prod_{p|m} 2 \leq \sqrt{D} \prod_{p|m} 2 = \sqrt{D} \cdot 2^{\omega(m)},$$

as claimed. □

3.2. **Proof of Theorem 1.4 and related remarks.** We now describe our adaptation of Hooley's argument [4] to the case of reducible quadratic polynomials, which culminates in a proof of Theorem 1.4. After the proof we make some additional comments on possible improvements to the theorem.

The only changes that need to be made to Hooley's argument [4] involve the differences in the function ρ_f resulting from the fact that f is now reducible. For one thing, the average size of ρ_f is now logarithmic rather than constant; this does not ruin the argument, but it needs to be taken into account. On the other hand, we know ρ_f much more exactly for reducible quadratic polynomials (as Lemma 3.3 shows) than we do for general irreducible polynomials; consequently, we are able to be more explicit in some stages. We also wish to make all dependencies on h and the polynomial f explicit in our upper bounds, for the benefit of anyone wishing to employ Theorem 1.4 in the future. Even so, the number of changes is small relative to the several-page length of Hooley's argument. We have therefore, with apologies to the reader, decided not to include a self-contained proof but rather to indicate the necessary alterations to Hooley's proof. We will use some of the notation therein without definition when defining the notation is superfluous to the current account.

Outline of proof of Theorem 1.4. We begin by examining Hooley's auxiliary lemmata from [4]. His Lemma 1–Lemma 3 are valid for any polynomial, reducible or irreducible, as the proofs essentially depend only on the Chinese remainder theorem. We will not use his Lemma 4–Lemma 6: these deal with various estimates for the function ρ_f, whereas we will simply use the information worked out earlier in this section. Finally, his Lemma 7–Lemma 8 make no reference to the polynomial and thus remain valid in our setting. (We note that since we are dealing always with quadratic polynomials, Hooley's parameters n and N will equal 2 and 4, respectively, for us.) For the remainder of this proof, we use x instead of y so as to conform with the notation in [4]; this is not to be confused with the x that appears in the rest of this paper.

Hooley's estimation proper of $R_f(h,x)$ begins with a certain decomposition [4, equation (1)], namely $R_f(h,x) = \Sigma_1 + \Sigma_2$, after which he observes that

$$\Sigma_2 \ll \sum_{\substack{k \leq x \\ k_1 > x^{1/3}}} \rho_f(k).$$

We employ the upper bound in Lemma 3.4 to deduce that

$$\Sigma_2 \ll \sqrt{D} \sum_{\substack{k \leq x \\ k_1 > x^{1/3}}} 2^{\omega(k)},$$

which differs from Hooley's estimate only in the presence of the $\sqrt{D}$ term. Thus no further changes are needed in the estimation of Σ_2: we obtain [4, equation (5)]

$$\Sigma_2 \ll \sqrt{D}\frac{x}{\log x},$$

which will turn out to be smaller than our estimate of Σ_1.

Subsequently, Hooley derives the upper bound [4, equations (6) and (7)]

$$\Sigma_1 \ll \sum_{k_1 \le x^{1/3}} \sqrt{\Sigma_5 \Sigma_6}.$$

In the estimation of Σ_5, the only modification we need to make is to include a factor of D in the estimate

$$\rho_f^2(k_2) \ll D \cdot 2^{2\omega(k_2)} \ll D \cdot d_4(k_2)$$

(the factor of D resulting from applying Lemma 3.4 as in the estimation of Σ_2). Hooley's majorization of Σ_6 is exactly suitable for our purposes, except that we wish to keep explicit the dependence on h, so that we use his equation (9) rather than his equation (10). Our resulting version of [4, equation (11)] is

$$\Sigma_1 \ll \sqrt{D}\frac{x(\log\log x)^{5/2}}{\log x} \sum_{k_1 \le x^{1/3}} \sqrt{\frac{2^{\omega(k_1)}(h,k_1)}{k_1\phi(k_1)}}.$$

As Hooley does, we extend the range of summation on the right-hand side to all $\ell \le x$ (the notation hides the fact that the sum currently runs over those integers less than x for which a certain divisor k_1 is at most $x^{1/3}$). The resulting sum is treated in Lemma 5.3 below, whence we obtain

$$\Sigma_1 \ll \sqrt{D}\frac{x(\log\log x)^{5/2}}{\log x} \cdot (\log x)^{\sqrt{2}} \prod_{p \mid h} \left(1 + \frac{7}{\sqrt{p}}\right).$$

This establishes the theorem. □

Theorem 1.4 gives the estimate $R_f(h,y) \ll_{f,h} y(\log y)^{\sqrt{2}-1}(\log\log y)^{5/2}$ for any nonzero integer h. On the other hand, the number of terms in the exponential sum is $\sum_{m \le y} \rho_f(m) \gg_f y \log y$ by equation (29) below. In other words, the exponential sum exhibits nontrivial cancellation for all nonzero h. By Weyl's criterion, this is precisely what is needed to show that the normalized roots of $f(t) \equiv 0 \pmod m$ are equidistributed modulo 1.

Note that for a linear polynomial $f(t) = at + b$ with $(a,b) = 1$, the normalized roots are not equidistributed modulo 1, since they cluster around the points $\frac{s}{a}$ with $(s,a) = 1$. A straightforward calculation and an invocation of Ramanujan's sum shows that

$$\sum_{k \le y} \sum_{\substack{a\nu + b \equiv 0 \pmod k \\ 0 < \nu \le k}} e^{2\pi i h\nu/k} = y\frac{\phi(a)}{a}\frac{\mu(a/(h,a))}{\phi(a/(h,a))} + O(h\log y),$$

which is the same order of magnitude as the number of summands y, at least for some values of h. On the other hand, the roots of the reducible quadratic $W(at+b)(ct+d)$ modulo m certainly include the roots of $at + b$ and $ct + d$, and so there will be a contribution to the exponential sum from these roots, whose order of magnitude is y. It seems reasonable to conjecture that the other

roots of the quadratic are distributed randomly. For example, with the polynomial $f(t) = t^2 - 1$, one would conjecture that

$$\sum_{k \le y} \sum_{\substack{\nu^2 - 1 \equiv 0 \pmod{k} \\ 0 < \nu \le k}} e^{2\pi i h \nu / k} = 2y + O_h(y^{1/2+\varepsilon}).$$

In any event, we should not expect any estimate of the form $R_f(h, y) = o(y)$ for reducible quadratic polynomials f; therefore the bound in Theorem 1.4 is not too far from what one could prove.

We remark that the dependence on D in the upper bound of Theorem 1.4 could be improved if necessary. There are two places in the proof of Theorem 1.4 where we use Lemma 3.4 to simply bound $\rho_f(n)$ by $\sqrt{D} \cdot 2^{\omega(n)}$; but for many values of n the true size of $\rho_f(n)$ is much closer to $2^{\omega(n)}$. A more precise application of Lemmas 3.1 and 3.3 would replace the $\sqrt{D}$ in Theorem 1.4 by a smaller multiplicative function of D, one that was $\ll_\varepsilon D^\varepsilon$, for instance. Similarly, the dependence of the upper bound on h could be slightly reduced by using the exact expression derived on the last line of equation (26) below.

4. Diophantine quadruples

With these two technical results in place, we can now proceed to the proof of Theorem 1.1. It turns out that the analysis hinges on studying a very specific family of Diophantine quadruples. A *doubly regular* Diophantine quadruple is one of the form

$$\{a, b, a + b + 2r, 4r(a + r)(b + r)\}, \tag{15}$$

where a, b, and r are positive integers satisfying $a < b$ and $ab + 1 = r^2$ (so that $\{a, b\}$ is a Diophantine pair); it is easy to verify that any such quadruple is in fact Diophantine. Let

$$Q(x) = \text{the number of doubly regular Diophantine quadruples contained in } [1, x].$$

Dujella proved that almost all Diophantine quadruples are doubly regular; more precisely, he showed [2, Section 4] that the number of Diophantine quadruples contained in $[1, x]$ is $Q(x) + O(x^{0.292} \log^2 x)$. Therefore it suffices to find an asymptotic formula for $Q(x)$.

Define the set

$$R(m) = \{\nu \colon 1 \le \nu \le m,\ \nu^2 \equiv 1 \pmod{m}\}.$$

Notice that in any doubly regular Diophantine quadruple, we have the congruence $r^2 = ab + 1 \equiv 1 \pmod{b}$. Moreover, the inequality $a < b$ forces $r \le b$ as well, so that r must be an element of $R(b)$. Conversely, any pair $\{r, b\}$ with $r \in R(b)$ gives rise to a doubly regular Diophantine quadruple by taking $a = (r^2 - 1)/b$, except that $r = 1$ gives rise to $a = 0$ which must be excluded. We must therefore count all the pairs $\{r, b\}$, with $r \in R(b) \setminus \{1\}$, such that the largest element $4r(a + r)(b + r)$ of the corresponding doubly regular Diophantine quadruple is at most x. In other words, if we define the function

$$L(a, r, b; x) = \begin{cases} 1, & \text{if } 4r(a + r)(b + r) \le x, \\ 0, & \text{otherwise,} \end{cases}$$

then

$$Q(x) = \sum_{b \in \mathbb{N}} \sum_{r \in R(b) \setminus \{1\}} L\left(\frac{r^2 - 1}{b}, r, b; x\right). \tag{16}$$

The obstacle we must overcome is this: whether or not $4r(a+r)(b+r) \le x$ depends heavily on where in the interval $[1,b]$ the congruential root r lies, when b is in the most significant range (around $x^{1/3}$ in size). By replacing the summand in equation (16) by upper and lower bounds, Dujella was able [2, Theorem 3] to work out that the order of magnitude of $Q(x)$, and hence of the number of Diophantine quadruples up to x, is $x^{1/3}\log x$. We use our knowledge of the equidistribution of the roots $r \in R(b)$ to show that $Q(x)$ is asymptotically the same as an analogous sum where the numbers r are chosen at random from $[1,b]$.

We use the notation $\rho(m) = \#R(m)$, which is a special case of the notation $\rho_g(m)$ from the last section with $g(t) = t^2 - 1$. Applying Lemma 3.3 to this polynomial shows that

$$\rho(p^\alpha) = \begin{cases} 2, & \text{if } p \neq 2 \text{ or } p^\alpha = 4, \\ 1, & \text{if } p^\alpha = 2, \\ 4, & \text{if } p = 2 \text{ and } \alpha \ge 3; \end{cases}$$

in particular,

$$\rho(m) = \left.\begin{cases} 2^{\omega(m)}, & \text{if } 2 \nmid m \text{ or } 2^2 \parallel m, \\ 2^{\omega(m)-1}, & \text{if } 2^1 \parallel m, \\ 2^{\omega(m)+1}, & \text{if } 2^3 \mid m \end{cases}\right\} \le 2^{\omega(m)+1}. \tag{17}$$

4.1. **Truncating the infinite sum.** To begin with, we need to truncate the infinite sum in equation (16) in a manageable way. It turns out that we can accomplish this by sorting doubly regular Diophantine quadruples by a rather than b.

Lemma 4.1. *For any real numbers $A, x \ge 2$, the number of doubly regular Diophantine quadruples* (15) *satisfying $a \le A$ and $4r(a+r)(b+r) \le x$ is $\ll (Ax)^{1/4}\log A$.*

Proof. As before, the congruence $r^2 = ab + 1 \equiv 1 \pmod a$ shows that r must be congruent to some $\nu \in R(a)$, so that we can write $r = \nu + ak$ for some integer k. Furthermore, the inequality $a < b$ forces $a < r$ as well, so that $k \ge 1$. Conversely, any such r determines a doubly regular Diophantine quadruple by taking $b = (r^2-1)/a$. Note that the inequality $4r(a+r)(b+r) \le x$ implies that

$$x \ge 4(\nu+ak)(a+\nu+ak)\left(\frac{(\nu+ak)^2-1}{a} + \nu + ak\right) > 4(ak)(ak)(ak^2) = 4a^3k^4;$$

in other words, it is necessary that $1 \le k < (x/4a^3)^{1/4}$. We conclude that for every integer a and every $\nu \in R(a)$, there are at most $(x/4a^3)^{1/4}$ corresponding doubly regular Diophantine quadruples contained in $[1,x]$. An upper bound for the number of such quadruples with $a \le A$ is therefore

$$\sum_{a\le A}\sum_{\nu\in R(a)}\left(\frac{x}{4a^3}\right)^{1/4} = \sum_{a\le A}\left(\frac{x}{4a^3}\right)^{1/4}\rho(a) \ll x^{1/4}\sum_{a<A}\frac{\rho(a)}{a^{3/4}} \ll x^{1/4}A^{1/4}\log A,$$

where the last step uses equation (30). □

Let $\psi(x) \ge 1$ be any function that tends to infinity as $x \to \infty$, but more slowly than $\log x$ (we will choose a specific function $\psi(x)$ later in equation (25)). The following proposition shows that we can truncate the sum in equation (16) at

$$B = B(x) = \lfloor x^{1/3}\psi(x)\rfloor. \tag{18}$$

Proposition 4.2. *For any real number $x \geq 3$,*

$$Q(x) = \sum_{b \leq B} \sum_{r \in R(b)} L\left(\frac{r^2-1}{b}, r, b; x\right) + O\left(x^{1/3}\left(\psi(x) + \frac{\log x}{\psi(x)^{1/2}}\right)\right),$$

where B is defined in equation (18)*.*

Proof. We begin by bounding the number of doubly regular Diophantine quadruples with $b > B$ and $4r(a+r)(b+r) \leq x$. Since $r^2 = ab+1$, these inequalities force $x \geq 4r(a+r)(b+r) > 4r^2 b > 4(ab)b > 4aB^2$; in other words, every such Diophantine quadruple satisfies $a < x/4B^2 \leq x^{1/3}/\psi(x)^2$. By Lemma 4.1, the number of such Diophantine quadruples is

$$\ll \left(\frac{x^{1/3}}{\psi(x)^2} \cdot x\right)^{1/4} \log\left(\frac{x^{1/3}}{\psi(x)^2}\right) \leq \frac{x^{1/3}\log x}{\psi(x)^{1/2}}.$$

Therefore equation (16) becomes

$$\begin{aligned} Q(x) &= \sum_{b \leq B} \sum_{r \in R(b)\setminus\{1\}} L\left(\frac{r^2-1}{b}, r, b; x\right) + O\left(\frac{x^{1/3}\log x}{\psi(x)^{1/2}}\right) \\ &= \sum_{b \leq B} \sum_{r \in R(b)} L\left(\frac{r^2-1}{b}, r, b; x\right) + O\left(B + \frac{x^{1/3}\log x}{\psi(x)^{1/2}}\right), \end{aligned}$$

which is equivalent to the statement of the proposition. □

4.2. **Invoking equidistribution.**

Lemma 4.3. *Let a, b, r be positive integers with $a < b$ and $ab+1 = r^2$. Then for any real number $x \geq 3$, the inequality $4r(a+r)(b+r) \leq x$ is equivalent to $\frac{r}{b} \leq \lambda(b,x)$, where*

$$\lambda(b,x) = \begin{cases} 1, & \text{if } b \leq (x/16)^{1/3}, \\ \sqrt{\dfrac{x^{1/2}}{2b^{3/2}} + \dfrac{1}{4}} - \dfrac{1}{2} + O\left(\dfrac{b}{x^{3/4}}\right), & \text{if } b > (x/16)^{1/3}. \end{cases} \tag{19}$$

Proof. The inequality $4r(a+r)(b+r) \leq x$ is the same as

$$\frac{r}{b}\left(\frac{r^2}{b^2} + \frac{r}{b} - \frac{1}{b^2}\right)\left(1 + \frac{r}{b}\right) \leq \frac{x}{4b^3}.$$

If we set $s = \frac{r}{b}$, which is the normalized root used in the statement of our equidistribution result, then this becomes

$$s^2(1+s)^2 \leq \frac{x}{4b^3} + \frac{s(1+s)}{b^2} = \frac{x}{4b^3}\left(1 + O\left(\frac{b}{x}\right)\right). \tag{20}$$

Note that $s \leq 1$ and so the left-hand side is at most 4. If it happens that $b \leq (x/16)^{1/3}$, then the first term on the right-hand side is at least 4, so that the inequality always holds; setting $\lambda(b,x) = 1$ is therefore valid in this region. Otherwise, for any positive real number y, we see by completing

the square that $s^2(1+s)^2 \le y$ if and only if $s \le (\sqrt{y}+1/4)^{1/2} - 1/2$. Using this equivalence, the inequality (20) becomes

$$\begin{aligned} s &\le \left(\sqrt{\frac{x}{4b^3} + \frac{s(1+s)}{b^2}} + \frac{1}{4}\right)^{1/2} - \frac{1}{2} \\ &= \left(\sqrt{\frac{x}{4b^3}\left(1 + O\left(\frac{b}{x}\right)\right)} + \frac{1}{4}\right)^{1/2} - \frac{1}{2} \\ &= \left(\sqrt{\frac{x}{4b^3}} + \frac{1}{4}\right)^{1/2}\left(1 + O\left(\frac{b}{x}\right)\right) - \frac{1}{2} \\ &= \left(\sqrt{\frac{x}{4b^3}} + \frac{1}{4}\right)^{1/2} - \frac{1}{2} + O\left(\frac{b}{x^{3/4}}\right), \end{aligned}$$

since $b \ge 1$. This establishes the lemma in the case where $b > (x/16)^{1/3}$. □

Proposition 4.4. *For any real number $x \ge 3$,*

$$Q(x) = \sum_{b \le B} \rho(b)\lambda(b,x) + O\left(x^{1/3}\psi(x)(\log x)^{\sqrt{2}/2}(\log\log x)^{5/4} + \frac{x^{1/3}\log x}{\psi(x)^{1/2}}\right),$$

where B is defined in equation (18)*.*

Proof. Consider the concatenation of B finite sequences, the bth of which consists of the roots of $t^2 \equiv 1 \pmod b$ normalized by dividing by b; in other words, consider the sequence $R(1) \cup \frac{1}{2}R(2) \cup \frac{1}{3}R(3) \cup \cdots \cup \frac{1}{B}R(B)$. This sequence has $S(B)$ elements, where we define

$$S(y) = \sum_{b \le y} \rho(b).$$

We will apply the moving-target Erdős-Turán inequality, Theorem 1.2, to this sequence; our target intervals will be $[0, \lambda(b,x)]$ for each element r/b of $\frac{1}{b}R(b)$. With this setup, we have

$$Z_{S(B)} = \sum_{b \le B} \#\{r \in R(b) \colon 0 \le \tfrac{r}{b} \le \lambda(b,x)\} = \sum_{b \le B} \sum_{r \in R(b)} L\left(\frac{r^2-1}{b}, r, b; x\right)$$

by Lemma 4.3, whence

$$D_{S(B)} = \sum_{b \le B} \sum_{r \in R(b)} L\left(\frac{r^2-1}{b}, r, b; x\right) - \sum_{b \le B} \rho(b)(\lambda(b,x) - 0).$$

In other words,

$$Q(x) = \sum_{b \le B} \rho(b)\lambda(b,x) + O\left(D_{S(B)} + x^{1/3}\left(\psi(x) + \frac{\log x}{\psi(x)^{1/2}}\right)\right)$$

by Proposition 4.2 (recalling that B is defined in equation (18)).

Our intervals $[0, \lambda(b,x)]$ have the property that the lower and upper endpoints each form monotone sequences; the variation in the lower endpoint is 0, while the variation in the upper endpoint

is $1-\lambda(B,x)\le 1$. By Corollary 1.3, we therefore have

$$D_{S(B)} \ll \frac{S(B)}{H} + \big(1+0+1\big)\sum_{h=1}^{H} M_{S(B)}(h) \ll \frac{S(B)}{H} + \sum_{h=1}^{H} M_{S(B)}(h)$$

for any positive integer H; we will choose H later in (22). By Lemma 5.5, the first term satisfies

$$\frac{S(B)}{H} \ll \frac{B\log B}{H} \ll \frac{x^{1/3}\psi(x)\log x}{H}.$$

By Theorem 1.4 applied with $y \le B$ and with $f(t)=t^2-1$, so that $D=2$,

$$M_{S(B)}(h) \ll \prod_{p\mid h}\left(1+\frac{7}{\sqrt{p}}\right)\cdot B(\log B)^{\sqrt{2}-1}(\log\log B)^{5/2} + \max_{1\le b\le B}\rho(b),$$

the final term arising because we have to consider what happens if we chop off the exponential sum in the middle of one of the finite sequences $\frac{1}{b}R(b)$; here even the crude bound $\rho(b)\le B$ suffices. Consequently, by Lemma 5.4 we have

$$\sum_{h\le H} M_{S(B)}(h) \ll HB(\log B)^{\sqrt{2}-1}(\log\log B)^{5/2}.$$

We conclude that

$$\begin{aligned} Q(x) &= \sum_{b\le B}\rho(b)\lambda(b,x) + O\bigg(\frac{x^{1/3}\psi(x)\log x}{H} + HB(\log B)^{\sqrt{2}-1}(\log\log B)^{5/2} + x^{1/3}\Big(\psi(x)+\frac{\log x}{\psi(x)^{1/2}}\Big)\bigg)\\ &= \sum_{b\le B}\rho(b)\lambda(b,x) + O\bigg(\frac{x^{1/3}\psi(x)\log x}{H} + Hx^{1/3}\psi(x)(\log x)^{\sqrt{2}-1}(\log\log x)^{5/2} + \frac{x^{1/3}\log x}{\psi(x)^{1/2}}\bigg). \end{aligned} \tag{21}$$

To optimize this error term, we choose H so that the first two terms are the same size. This choice turns out to be

$$H = \big\lceil (\log x)^{1-\sqrt{2}/2}(\log\log x)^{-5/4}\big\rceil, \tag{22}$$

and with this choice, we get

$$Q(x) = \sum_{b\le B}\rho(b)\lambda(b,x) + O\bigg(x^{1/3}\psi(x)(\log x)^{\sqrt{2}/2}(\log\log x)^{5/4} + \frac{x^{1/3}\log x}{\psi(x)^{1/2}}\bigg).$$

□

4.3. **Calculating the weighted sum.** We evaluate the sum

$$\sum_{b\le B}\rho(b)\lambda(b,x)$$

by partial summation, recalling that $B=\lfloor x^{1/3}\psi(x)\rfloor$ where $\psi(x)$ tends to infinity but more slowly than $\log x$; we also recall the notation $S(y)=\sum_{b\le y}\rho(b)$. After working hard to evaluate the eventual leading constant in closed form, we finally finish the proof of Theorem 1.1 at the end of this section.

Proposition 4.5. *For any real number $x \geq 3$,*

$$\sum_{b\leq B} \rho(b)\lambda(b,x) = \frac{3x^{1/2}}{4}\int_{(x/16)^{1/3}}^{\infty} \left(1+\frac{2x^{1/2}}{t^{3/2}}\right)^{-1/2} \frac{S(t)}{t^{5/2}}\,dt + O\left(\frac{x^{1/3}\log x}{\psi(x)^{1/2}}\right).$$

Proof. For notational convenience in this proof, we set $B_1 = (x/16)^{1/3}$. Using the definition (19) of $\lambda(b,x)$, we have

$$\begin{aligned}\sum_{b\leq B} \rho(b)\lambda(b,x) &= \sum_{b\leq B_1}\rho(b) + \sum_{B_1<b\leq B}\rho(b)\left(\sqrt{\frac{x^{1/2}}{2b^{3/2}}+\frac{1}{4}} - \frac{1}{2} + O\left(\frac{b}{x^{3/4}}\right)\right)\\ &= S(B_1) + \sum_{B_1<b\leq B}\rho(b)\sqrt{\frac{x^{1/2}}{2b^{3/2}}+\frac{1}{4}} - \tfrac{1}{2}(S(B)-S(B_1)) + O\left(\frac{B}{x^{3/4}}S(B)\right)\\ &= \sum_{B_1<b\leq B}\rho(b)\sqrt{\frac{x^{1/2}}{2b^{3/2}}+\frac{1}{4}} + \tfrac{3}{2}S(B_1) - \tfrac{1}{2}S(B) + O(1). \end{aligned} \tag{23}$$

The remaining sum can be written as a Riemann-Stieltjes integral, to which integration by parts can be applied:

$$\begin{aligned}\sum_{B_1<b\leq B}\rho(b)\sqrt{\frac{x^{1/2}}{2b^{3/2}}+\frac{1}{4}} &= \int_{B_1}^{B}\left(\frac{x^{1/2}}{2t^{3/2}}+\frac{1}{4}\right)^{1/2} dS(t)\\ &= S(B)\left(\frac{x^{1/2}}{2B^{3/2}}+\frac{1}{4}\right)^{1/2} - S(B_1)\left(\frac{x^{1/2}}{2B_1^{3/2}}+\frac{1}{4}\right)^{1/2}\\ &\quad - \int_{B_1}^{B} S(t)\frac{d}{dt}\left(\frac{x^{1/2}}{2t^{3/2}}+\frac{1}{4}\right)^{1/2} dt. \end{aligned} \tag{24}$$

We note that

$$\left(\frac{x^{1/2}}{2B^{3/2}}+\frac{1}{4}\right)^{1/2} = \left(\frac{1}{2\psi(x)^{3/2}}+\frac{1}{4}\right)^{1/2} = \frac{1}{2} + O\left(\frac{1}{\psi(x)^{3/2}}\right),$$

while the similar term with B replaced by B_1 evaluates to exactly $\frac{3}{2}$; we also note that

$$\frac{d}{dt}\left(\frac{x^{1/2}}{2t^{3/2}}+\frac{1}{4}\right)^{1/2} = -\frac{3x^{1/2}}{8t^{5/2}}\left(\frac{x^{1/2}}{2t^{3/2}}+\frac{1}{4}\right)^{-1/2}.$$

Therefore equation (24) becomes

$$\sum_{B_1<b\leq B}\rho(b)\sqrt{\frac{x^{1/2}}{2b^{3/2}}+\frac{1}{4}} = \left(\tfrac{1}{2}+O(\psi(x)^{-3/2})\right)S(B) - \tfrac{3}{2}S(B_1) + \tfrac{3}{8}x^{1/2}\int_{B_1}^{B}\frac{S(t)}{t^{5/2}}\left(\frac{x^{1/2}}{2t^{3/2}}+\frac{1}{4}\right)^{-1/2} dt,$$

which results in a lot of cancellation in equation (23):

$$\begin{aligned}\sum_{b\leq B}\rho(b)\lambda(b,x) &= \tfrac{3}{8}x^{1/2}\int_{B_1}^{B}\frac{S(t)}{t^{5/2}}\left(\frac{x^{1/2}}{2t^{3/2}}+\frac{1}{4}\right)^{-1/2} dt + O\left(\frac{S(B)}{\psi(x)^{3/2}}\right)\\ &= \tfrac{3}{4}x^{1/2}\int_{B_1}^{B}\frac{S(t)}{t^{5/2}}\left(\frac{2x^{1/2}}{t^{3/2}}+1\right)^{-1/2} dt + O\left(\frac{B\log B}{\psi(x)^{3/2}}\right)\end{aligned}$$

by Lemma 5.5. Finally, we extend the integral to infinity, noting that

$$\int_B^\infty \frac{S(t)}{t^{5/2}}\left(\frac{2x^{1/2}}{t^{3/2}}+1\right)^{-1/2} dt \ll \int_B^\infty \frac{t\log t}{t^{5/2}} = 2B^{-1/2}\log B + 4B^{-1/2} \ll \frac{\log B}{B^{1/2}},$$

so that

$$\sum_{b\le B}\rho(b)\lambda(b,x) = \tfrac{3}{4}x^{1/2}\int_{B_1}^\infty \frac{S(t)}{t^{5/2}}\left(\frac{2x^{1/2}}{t^{3/2}}+1\right)^{-1/2} dt + O\left(\frac{B\log B}{\psi(x)^{3/2}} + \frac{x^{1/2}\log B}{B^{1/2}}\right).$$

Since $B = \lfloor x^{1/3}\psi(x)\rfloor$, both error terms are $\ll x^{1/3}(\log x)/\psi(x)^{1/2}$, which establishes the proposition. □

Lemma 4.6. *For any real number $x \ge 3$,*

$$\frac{3x^{1/2}}{4}\int_{(x/16)^{1/3}}^\infty \left(1+\frac{2x^{1/2}}{t^{3/2}}\right)^{-1/2}\frac{S(t)}{t^{5/2}}\,dt = \frac{2^{2/3}}{\pi^2}x^{1/3}\log x\int_0^1 (1+8u)^{-1/2}u^{-2/3}\,du + O(x^{1/3}).$$

Proof. First we use the asymptotic formula for $S(t)$ in Lemma 5.5:

$$\begin{aligned}&\int_{(x/16)^{1/3}}^\infty \left(1+\frac{2x^{1/2}}{t^{3/2}}\right)^{-1/2}\frac{S(t)}{t^{5/2}}\,dt\\ &\qquad = \frac{6}{\pi^2}\int_{(x/16)^{1/3}}^\infty \left(1+\frac{2x^{1/2}}{t^{3/2}}\right)^{-1/2}\frac{\log t}{t^{3/2}}\,dt + O\left(\int_{(x/16)^{1/3}}^\infty \left(1+\frac{2x^{1/2}}{t^{3/2}}\right)^{-1/2}\frac{1}{t^{3/2}}\,dt\right).\end{aligned}$$

Since $(1+2x^{1/2}/t^{3/2})^{-1/2} < 1$, the last integral is bounded above by $2((x/16)^{1/3})^{-1/2}$. Therefore

$$\frac{3x^{1/2}}{4}\int_{(x/16)^{1/3}}^\infty \left(1+\frac{2x^{1/2}}{t^{3/2}}\right)^{-1/2}\frac{S(t)}{t^{5/2}}\,dt = \frac{9x^{1/2}}{2\pi^2}\int_{(x/16)^{1/3}}^\infty \left(1+\frac{2x^{1/2}}{t^{3/2}}\right)^{-1/2}\frac{\log t}{t^{3/2}}\,dt + O(x^{1/3}).$$

We now make the change of variables $u = x^{1/2}/4t^{3/2}$ in the remaining integral, which yields

$$\begin{aligned}&\frac{9x^{1/2}}{2\pi^2}\int_{(x/16)^{1/3}}^\infty \left(1+\frac{2x^{1/2}}{t^{3/2}}\right)^{-1/2} t^{-3/2}\log t\,dt\\ &\qquad = \frac{9x^{1/2}}{2\pi^2}\int_1^0 (1+8u)^{-1/2}\frac{4u}{x^{1/2}}\log\frac{x^{1/3}}{2^{4/3}u^{2/3}}\left(-\frac{x^{1/3}}{3\cdot 2^{1/3}u^{5/3}}\,du\right)\\ &\qquad = \frac{2^{2/3}x^{1/3}}{\pi^2}\left((\log x)\int_0^1 (1+8u)^{-1/2}u^{-2/3}\,du + 2\int_0^1 (1+8u)^{-1/2}\frac{\log 4u}{u^{2/3}}\,du\right)\end{aligned}$$

This establishes the lemma, on noting that the last integral converges to some finite constant. □

Lemma 4.7. *We have*

$$\frac{2^{2/3}}{\pi^2}\int_0^1 (1+8u)^{-1/2}u^{-2/3}\,du = \frac{2^{4/3}}{3\Gamma(\frac{2}{3})^3} \approx 0.338285.$$

Proof. This lemma turns out to be an exercise in mining known results about special functions. We begin with Euler's integral representation [1, equation (15.3.1)] for the hypergeometric function

${}_2F_1$, valid for all complex numbers z other than real numbers greater than or equal to 1, as long as $\Re c > \Re b > 0$:

$$ {}_2F_1(a,b;c;z) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)} \int_0^1 t^{b-1}(1-t)^{c-b-1}(1-tz)^{-a}\,dt $$

Choosing $a = \frac{1}{2}$, $b = \frac{1}{3}$, $c = \frac{4}{3}$, and $z = -8$, and recalling that $\Gamma(y+1) = y\Gamma(y)$, we see that

$$ \frac{2^{2/3}}{\pi^2} \int_0^1 (1+8u)^{-1/2} u^{-2/3}\,du = \frac{2^{2/3}}{\pi^2} \frac{\Gamma(\frac{1}{3})\Gamma(1)}{\Gamma(\frac{4}{3})} {}_2F_1\big(\tfrac{1}{2},\tfrac{1}{3};\tfrac{4}{3};-8\big) = \frac{3\cdot 2^{2/3}}{\pi^2} {}_2F_1\big(\tfrac{1}{2},\tfrac{1}{3};\tfrac{4}{3};-8\big). $$

Next, we apply the quadratic transformation [1, equation (15.3.22)]

$$ {}_2F_1\big(a,b;a+b+\tfrac{1}{2};z\big) = {}_2F_1\big(2a,2b;a+b+\tfrac{1}{2};\tfrac{1}{2}-\tfrac{1}{2}\sqrt{1-z}\big) $$

to obtain

$$ \frac{3\cdot 2^{2/3}}{\pi^2} {}_2F_1\big(\tfrac{1}{2},\tfrac{1}{3};\tfrac{4}{3};-8\big) = \frac{3\cdot 2^{2/3}}{\pi^2} {}_2F_1\big(1,\tfrac{2}{3};\tfrac{4}{3};-1\big). $$

At this point, we can actually evaluate this special value by the formula [1, equation (15.1.21)]

$$ {}_2F_1(a,b;a-b+1;-1) = 2^{-a}\pi^{1/2} \frac{\Gamma(1+a-b)}{\Gamma(1+\frac{a}{2}-b)\Gamma(\frac{1}{2}+\frac{a}{2})}, $$

which gives

$$ \frac{3\cdot 2^{2/3}}{\pi^2} {}_2F_1\big(1,\tfrac{2}{3};\tfrac{4}{3};-1\big) = \frac{3}{2^{1/3}\pi^{3/2}} \frac{\Gamma(\frac{4}{3})}{\Gamma(\frac{5}{6})\Gamma(1)} = \frac{1}{2^{1/3}\pi^{3/2}} \frac{\Gamma(\frac{1}{3})}{\Gamma(\frac{5}{6})}. $$

We now invoke the duplication formula for the Gamma function [1, equation (6.1.18)], namely $\Gamma(2z) = (2\pi)^{-1/2} 2^{2z-1/2} \Gamma(z)\Gamma\big(z+\frac{1}{2}\big)$. At $z = \frac{1}{3}$ this yields $\Gamma(\frac{5}{6}) = 2^{1/3}\pi^{1/2}\Gamma(\frac{2}{3})/\Gamma(\frac{1}{3})$, so that

$$ \frac{1}{2^{1/3}\pi^{3/2}} \frac{\Gamma(\frac{1}{3})}{\Gamma(\frac{5}{6})\Gamma(1)} = \frac{1}{2^{2/3}\pi^2} \frac{\Gamma(\frac{1}{3})^2}{\Gamma(\frac{2}{3})} $$

Finally, the reflection formula for the Gamma function [1, equation (6.1.17)] is $\Gamma(z)\Gamma(1-z) = \pi \csc \pi z$; again choosing $z = \frac{1}{3}$, we obtain $\Gamma(\frac{1}{3}) = \pi \csc \frac{\pi}{3}/\Gamma(\frac{2}{3}) = 2\pi/3^{1/2}\Gamma(\frac{2}{3})$, so that

$$ \frac{1}{2^{2/3}\pi^2} \frac{\Gamma(\frac{1}{3})^2}{\Gamma(\frac{2}{3})} = \frac{2^{4/3}}{3\Gamma(\frac{2}{3})^3} $$

This chain of equalities establishes the lemma. □

Proof of Theorem 1.1. By Proposition 4.4,

$$ Q(x) = \sum_{b\le B} \rho(b)\lambda(b,x) + O\bigg(x^{1/3}\psi(x)(\log x)^{\sqrt{2}/2}(\log\log x)^{5/4} + \frac{x^{1/3}\log x}{\psi(x)^{1/2}} \bigg). $$

By Proposition 4.5,

$$ Q(x) = \frac{3x^{1/2}}{4} \int_{(x/16)^{1/3}}^{\infty} \bigg(1+\frac{2x^{1/2}}{t^{3/2}}\bigg)^{-1/2} \frac{S(t)}{t^{5/2}}\,dt + O\bigg(x^{1/3}\psi(x)(\log x)^{\sqrt{2}/2}(\log\log x)^{5/4} + \frac{x^{1/3}\log x}{\psi(x)^{1/2}} \bigg). $$

At this point we choose

$$ \psi(x) = (\log x)^{(2-\sqrt{2})/3}(\log\log x)^{-5/6} \tag{25} $$

to optimize the error term, yielding

$$Q(x) = \frac{3x^{1/2}}{4} \int_{(x/16)^{1/3}}^{\infty} \left(1 + \frac{2x^{1/2}}{t^{3/2}}\right)^{-1/2} \frac{S(t)}{t^{5/2}}\, dt + O\big(x^{1/3}(\log x)^{2/3+\sqrt{2}/6}(\log\log x)^{5/12}\big).$$

By Lemma 4.6,

$$Q(x) = \frac{2^{2/3}}{\pi^2} x^{1/3} \log x \int_0^1 (1+8u)^{-1/2} u^{-2/3}\, du + O\big(x^{1/3}(\log x)^{2/3+\sqrt{2}/6}(\log\log x)^{5/12}\big).$$

Finally, by Lemma 4.7,

$$Q(x) = \frac{2^{4/3}}{3\Gamma(\frac{2}{3})^3} x^{1/3} \log x + O\big(x^{1/3}(\log x)^{2/3+\sqrt{2}/6}(\log\log x)^{5/12}\big).$$

□

5. Sums of multiplicative functions

In this section we gather together the facts about sums of multiplicative functions that we used in Sections 3 and 4. All of the specific results we need are special cases of the following asymptotic formula, several variants of which have appeared in the literature.

Proposition 5.1. *Let $g(n)$ be a nonnegative multiplicative function. Suppose that there exist real numbers U and κ such that $g(p^\alpha) \le U$ for all prime powers p^α and*

$$\sum_{p \le w} \frac{g(p)\log p}{p} = \kappa \log w + O_g(1)$$

for all $w \ge 2$. Then the asymptotic formula

$$\sum_{n \le y} \frac{g(n)}{n} = c(g) \log^\kappa y + O_g(\log^{\kappa-1} y)$$

holds for all $y \ge 2$, where $c(g)$ is the convergent product

$$c(g) = \frac{1}{\Gamma(\kappa+1)} \prod_p \left(1 - \frac{1}{p}\right)^\kappa \left(1 + \frac{g(p)}{p} + \frac{g(p^2)}{p^2} + \cdots\right).$$

Proof. This is exactly [6, Proposition A.3(a)], except that we have replaced the hypothesis "$g(n) \ll n^\alpha$ for some constant $\alpha < 1/2$" with "there exists U such that $g(p^\alpha) \le U$ for all prime powers p^α". This is a strictly stronger hypothesis, however: any nonnegative multiplicative function satisfying $g(p^\alpha) \le U$ automatically satisfies $g(n) \le U^{\omega(n)} \ll_{U,\varepsilon} n^\varepsilon$ for every $\varepsilon > 0$. □

In the following lemmas we use the standard notations $\phi(n)$ for the Euler phi-function, $\mu(n)$ for the Möbius mu-function, and $\omega(n)$ for the number of distinct prime divisors of n. Note that μ^2 is the characteristic function of the squarefree integers.

Lemma 5.2. *For all $y \ge 2$, we have* $\displaystyle\sum_{n \le y} \sqrt{\frac{2^{\omega(n)}}{n\phi(n)}} \ll (\log y)^{\sqrt{2}}$.

Proof. Define the multiplicative function

$$g(n) = \sqrt{\frac{n2^{\omega(n)}}{\phi(n)}} = \prod_{p|n} \sqrt{\frac{2p}{p-1}},$$

so that the sum we need to estimate is $\sum_{n\le y} g(n)/n$. We note that $g(p^\alpha) = \sqrt{2p/(p-1)} \le 2$ for all prime powers p^α, and we evaluate

$$\begin{aligned}
\sum_{p\le y} \frac{g(p)\log p}{p} &= \sum_{p\le y} \sqrt{\frac{2p}{p-1}}\frac{\log p}{p} \\
&= \sqrt{2}\sum_{p\le y} \frac{\log p}{p\sqrt{1-1/p}} \\
&= \sqrt{2}\sum_{p\le y} \frac{\log p}{p}\left(1 + O\left(\frac{1}{p}\right)\right) \\
&= \sqrt{2}\sum_{p\le y} \frac{\log p}{p} + O\bigg(\sum_{p\le y} \frac{\log p}{p^2}\bigg) \\
&= \sqrt{2}\log y + O(1).
\end{aligned}$$

Proposition 5.1 therefore applies with $\kappa = \sqrt{2}$, yielding

$$\sum_{n\le y} \sqrt{\frac{2^{\omega(n)}}{n\phi(n)}} = \sum_{n\le y} \frac{g(n)}{n} = c(g)(\log y)^{\sqrt{2}} + O_g((\log y)^{\sqrt{2}-1}) \ll (\log y)^{\sqrt{2}}$$

as claimed (the $\ll$-constant is absolute since the function g is fixed). □

Lemma 5.3. *For all $y \ge 2$ and for any nonzero integer h,*

$$\sum_{n\le y} \sqrt{\frac{2^{\omega(n)}(h,n)}{n\phi(n)}} \ll (\log y)^{\sqrt{2}} \prod_{p|h} \left(1 + \frac{7}{\sqrt{p}}\right)$$

Proof. We sort the integers $n \le y$ according to their greatest common divisor d with h:

$$\sum_{n\le y} \sqrt{\frac{2^{\omega(n)}(h,n)}{n\phi(n)}} = \sum_{d|h} \sqrt{d} \sum_{\substack{n\le y \\ (n,h)=d}} \sqrt{\frac{2^{\omega(n)}}{n\phi(n)}} = \sum_{d|h} \sqrt{d} \sum_{\substack{m\le y/d \\ (m,h)=1}} \sqrt{\frac{2^{\omega(dm)}}{dm\phi(dm)}}.$$

The condition $(m,h)=1$ implies that $(m,d)=1$, and so

$$\sum_{n\le y} \sqrt{\frac{2^{\omega(n)}(h,n)}{n\phi(n)}} = \sum_{d|h} \sqrt{\frac{2^{\omega(d)}}{\phi(d)}} \sum_{\substack{m\le y/d \\ (m,h)=1}} \sqrt{\frac{2^{\omega(m)}}{m\phi(m)}} \le \sum_{d|h} \sqrt{\frac{2^{\omega(d)}}{\phi(d)}} \sum_{m\le y} \sqrt{\frac{2^{\omega(m)}}{m\phi(m)}}.$$

The inner sum is $\ll (\log y)^{\sqrt{2}}$ by Lemma 5.2, and so it remains to bound the sum over d. But this is a multiplicative function of h, and so

$$\begin{aligned}\sum_{d|h}\sqrt{\frac{2^{\omega(d)}}{\phi(d)}} &= \prod_{p^\alpha\|h}\Big(1+\sqrt{\frac{2^{\omega(p)}}{\phi(p)}}+\cdots+\sqrt{\frac{2^{\omega(p^\alpha)}}{\phi(p^\alpha)}}\Big)\\ &= \prod_{p^\alpha\|h}\Big(1+\sqrt{\frac{2}{p-1}}+\cdots+\sqrt{\frac{2}{p^{r-1}(p-1)}}\Big)\\ &= \prod_{p^\alpha\|h}\Big(1+\sqrt{\frac{2}{p-1}}\sum_{j=0}^{r-1}\frac{1}{p^{j/2}}\Big)\\ &\le \prod_{p|h}\Big(1+\sqrt{\frac{2}{p-1}}\big(1-p^{-1/2}\big)^{-1}\Big). \qquad (26)\end{aligned}$$

The lemma follows upon verifying that $\sqrt{2/(p-1)}(1-p^{-1/2})^{-1}\le 7/\sqrt{p}$ for all $p\ge 2$. □

For certain multiplicative functions g, we can actually find an asymptotic formula not just for $\sum_{m\le y} g(m)/m$ but also for $\sum_{m\le y} g(m)$. In our next lemma we record only the upper bound, even though we can derive an asymptotic formula; in the lemma after that, the asymptotic formula is important enough to retain.

Lemma 5.4. *For all $y\ge 2$, we have $\displaystyle\sum_{m\le y}\prod_{p|m}\Big(1+\frac{7}{\sqrt{p}}\Big)\ll y$.*

Proof. Define the multiplicative function $g(m)=7^{\omega(m)}\mu^2(m)/\sqrt{m}$, where μ is the Möbius mu-function. One can check that

$$\prod_{p|m}\Big(1+\frac{7}{\sqrt{p}}\Big)=\sum_{d|m}g(d)$$

(because both sides are multiplicative functions of m, it suffices to check the equality on prime powers). We have

$$\sum_{m\le y}\prod_{p|m}\Big(1+\frac{7}{\sqrt{p}}\Big)=\sum_{m\le y}\sum_{d|m}g(d)=\sum_{d\le y}g(d)\sum_{\substack{m\le y\\ d|m}}1=y\sum_{d\le y}\frac{g(d)}{d}+O\Big(\sum_{d\le y}g(d)\Big). \qquad (27)$$

Since $g(m)\ll_\varepsilon m^{-1/2+\varepsilon}$ for any $\varepsilon>0$, the error term is $O_\varepsilon(y^{1/2+\varepsilon})$. We note that $g(p^\alpha)<7$ for all prime powers p^α, and we evaluate

$$\sum_{p\le y}\frac{g(p)\log p}{p}=\sum_{p\le y}\frac{7\log p}{p^{3/2}}\ll 1.$$

Proposition 5.1 therefore applies with $\kappa=0$, yielding

$$\sum_{d\le y}\frac{g(d)}{d}=c(g)+O_g((\log y)^{-1})\ll 1.$$

The proposition now follows from equation (27) and this last estimate. □

Lemma 5.5. *Define $S(y)=\sum_{b\le y}\rho(b)$. For all $y\ge 2$, we have $S(y)=\frac{6}{\pi^2}y\log y+O(y)$.*

Proof. Define the multiplicative function g by its values on prime powers as follows:

$$g(p^\alpha) = \mu^2(p^\alpha) \text{ for } p \text{ odd or } \alpha \geq 4; \qquad g(2) = 0,\ g(4) = 1,\ g(8) = 2.$$

As in the proof of the previous lemma, one can check that $\rho(m) = \sum_{d|m} g(d)$, and so

$$S(y) = y \sum_{d \leq y} \frac{g(d)}{d} + O\bigg(\sum_{d \leq y} g(d) \bigg). \tag{28}$$

Since g is bounded by 2, the error term is $O(y)$. We note that $g(p^\alpha) \leq 2$ for all prime powers p^α, and we evaluate

$$\sum_{p \leq y} \frac{g(p) \log p}{p} = \sum_{2 < p \leq y} \frac{\log p}{p} = \log y + O(1).$$

Proposition 5.1 therefore applies with $\kappa = 1$, yielding

$$\begin{aligned} \sum_{d \leq y} \frac{g(d)}{d} &= \log y \bigg(1 - \frac{1}{2}\bigg)\bigg(1 + \frac{0}{2} + \frac{1}{4} + \frac{2}{8}\bigg) \prod_{p > 2} \bigg(1 - \frac{1}{p}\bigg)\bigg(1 + \frac{1}{p}\bigg) + O_g(1) \\ &= \log y \prod_p \bigg(1 - \frac{1}{p^2}\bigg) + O(1) = \frac{\log y}{\zeta(2)} + O(1) = \frac{6}{\pi^2} \log y + O(1). \end{aligned}$$

The proposition now follows from equation (28) and this last asymptotic formula. □

When ρ is generalized to ρ_f for any reducible, nonsquare quadratic polynomial f with integer coefficients, the proof of Lemma 5.5 generalizes to yield

$$\sum_{m \leq y} \rho_f(m) = c(f) y \log y + O_f(y) \tag{29}$$

for some positive constant $c(f)$. It is also easy to show (by splitting the sum into dyadic intervals, for example) that

$$\sum_{a \leq A} \frac{\rho(a)}{a^{3/4}} \ll A^{1/4} \log A. \tag{30}$$

Acknowledgements. We thank John Friedlander, Roger Heath-Brown, and Hugh Montgomery for their insights into the work of Erdős–Turán and Hooley.

REFERENCES

[1] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, Dover Publications Inc., New York (1965).
[2] A. Dujella, "On the number of Diophantine m-tuples", *Ramanujan J.* **15** (2008), no. 1, 37–46.
[3] A. Dujella, "There are only finitely many Diophantine quintuples", *J. Reine Angew. Math.* **566** (2004), 183–214.
[4] C. Hooley, "On the distribution of the roots of polynomial congruences", *Mathematika* **11** (1964), 39–49.
[5] C. Hooley, "On the number of divisors of quadratic congruences", *Acta. Math.* **110** (1963), 97–114.
[6] G. Martin, "An asymptotic formula for the number of smooth values of a polynomial", *J. Number Theory* **93** (2002), no. 2, 108–182.
[7] H. L. Montgomery, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS Regional Conference Series in Mathematics, 84, American Mathematical Society, Providence, RI (1994).
[8] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition, John Wiley & Sons, Inc., New York (1991).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, ROOM 121, 1984 MATHEMATICS ROAD, CANADA V6T 1Z2

E-mail address: gerg@math.ubc.ca and sesitar@math.ubc.ca